REMARKS

The Final Office Action, mailed November 10, 2008, considered claims 1 and 3-37. Claims 1, 3-11 and 22-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable by Goldberg et al. (U.S. Patent Application Publication No. 20040013112) in view of Wilson et al. (U.S. Patent No. 7159119), and further in view of Hunt et al. (U.S. Patent Application Publication No. 20030005306). Claims 12-17, 19-21, 29-32 and 34-37 were rejected under 35 U.S.C. § 103(a) as being unpatentable by Goldberg et al. (U.S. Pat. Pub. No. 20040013112), in view of Wilson et al. (U.S. Patent 7,159,119).[1]

By this response, claims 1, 4, 9-10, 12-13, 15, 20-23, 27-30, 35 and 36 are amended, while claims 18 and 33 are cancelled, such that claims 1, 3-17, 18-32 and 34-37 remain pending.[2] Claims 1, 12, 22 and 29 are independent claims which remain at issue. Support for the amendments is found throughout the specification, including, but not limited to the disclosure found in ¶¶ 0009, 0012-0013, 0029, 0031 and 0044-0045.[3]

The present invention is generally directed to embodiments for preventing denial of service ("DoS") attacks on a server without significantly affecting performance. In summary, embodiments provide a first hashing function and a first table of verified remote entities, as well as a second cryptographically secure hashing function and a second table of unverified remote entities. The dual tables and hashing functions allow a server to use the first hashing function when it encounters packets from a verified entity, and the second hashing function only when it encounters packets from an unverified entity. Doing so protects the server from a DoS attack by preventing it from indexing state information for malicious packets to an identical index in a single table, reducing performance.

For example, claim 1 recites a method in which a local server receives a packet of data from a remote entity that includes connection identifier information. The server hashes at least a portion of the connection identifier information using a first hash function, generating a first hash. The first hash identifies an entry in a first table of verified remote entities, which stores remote entities that have a confirmed connection identifier.

---

[1] Although the prior art status of the cited art is not being specifically challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

[2] The amendments and remarks presented herein are consistent with that discussed by telephone by patent attorney Thomas M. Bonacci (reg. no. 63,368).

[3] Paragraph references refer to the application as originally filed.

When it is determined that state information for the remote entity exists at the entry in the first table of verified remote entities, standard data transport protocol is performed on the packet of data.

When it is determined that state information for the remote entity does not exist in the first table of verified remote entities, the server hashes at least a portion of the connection identifier information using a second hash function that is cryptographically secure to generate a second hash. The second hash function has a lower probability than the first hash function of generating an identical hash for connection identifier information from multiple remote entities. The second hash identifies a second entry in a second table of unverified remote entities, which stores remote entities that do not have a confirmed connection identifier.

When it is determined that state information for the remote entity exists at the second entry in the second table of unverified remote entities, the server compares secret information provided within the packet of data to information previously supplied to the remote entity to determine if the remote entity can be verified. When verified, the state information can be moved to the first table of verified remote entities.

When it is determined that state information for the remote entity does not exist in the second table of unverified remote entities, the server determines whether it is a listener that may accept the packet of data from the remote entity; if so, it is determined when the state information for the remote entity should be created in the second table of unverified remote entities.

Claim 12 recites a method similar to that of claim 1, but it includes functional 'step for' language. Claims 22 and 29 are directed to computer program products comprising computer readable storage media storing computer executable instructions for implementing the methods of claims 1 and 12 respectively.

Claims 1, 18, 22 and 33 were rejected under 35 U.S.C. 112, ¶ 2 as "being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention." In particular, the Examiner rejected to the limitation of "a second hash function that is more computationally intensive and more cryptographically secure than the first hash function." (*see* ¶ 9 of the Office Action). As amended, the claims particularly point out and distinctly claim that "the second [cryptographically secure] hash function [has] a lower probability than the first hash function

of generating an identical hash for connection identifier information from more than one remote entity."

Claims 1, 3-11 and 22-28 were rejected as being obvious in view of the combination of Goldberg, Wilson and Hunt, while claims 12, 17, 19-21, 29-32 and 34-37 were rejected as being obvious in view of the combination of Goldberg and Wilson. In view of the current amendments, however, Applicant submits that these references fail to teach or suggest each limitation of the independent claims and corresponding dependent claims.

Goldberg is generally directed to embodiments for implementing a firewall or packet filter to monitor the state of a communications session (*see, e.g.,* Goldberg, Abstract and ¶ 0014). Goldberg uses a hash function to hash socket information, and then stores session related data and parameters in a single session database, which facilitates quick lookups of session information for a packet (*see, e.g.,* Goldberg ¶¶ 0061-0062, 0066-0067, and 0071). Two hashing functions may be used, the first when full socket information is known, and the second when only partial socket information is known (*see, e.g.,* Goldberg ¶ 0014). The second hashing function is used to allow temporary openings in the firewall, facilitating dynamic filtering (*see, e.g.,* Goldberg ¶ 0085).

However, Goldberg fails to teach or suggest "a first [hash] table of verified remote entities, the first table for storing remote entities that have a confirmed connection identifier" and "a second [hash] table of unverified remote entities, the second table for storing remote entities that do not have a confirmed connection identifier," as recited by claims 1 and 12. Instead, Goldberg has a single session database.

Further, Goldberg fails to teach or suggest "a second hash function that is cryptographically secure," and especially when "the second hash function [has] a lower probability than the first hash function of generating an identical hash for connection identifier information from more than one remote entity," as recited by claims 1 and 12. Instead, Goldberg has two indistinguishable hashing functions.

Thus, Goldberg fails to teach or suggest storing a hash generated by the first hash function in the first table of verified entities and storing a hash generated by the second cryptographically secure hash function in the second table of unverified entities. This combination "prevent[s] denial of service attacks on lookup tables used to store state information for one or more remote entities, while

maintaining the performance of the local server for packets from verified remote entities" (see preamble, claims 1 and 12).

The other cited art, Wilson and Hunt, fail to compensate for the foregoing inadequacies of Goldberg. Wilson teaches that a secured database can manage multiple information types, and therefore use multiple look-up tables (*see*, Wilson, Abstract and col. 4, l. 50-54), while Hunt teaches that a cryptographic hash function can generate a relatively short but highly unique identifier and that a data backup application can use such an identifier to determine whether file contents have changed (*see*, Hunt ¶¶ 0027 and 0030). However, both Wilson and Hunt fail to teach or suggest the foregoing limitations, including "a first [hash] table of verified remote entities, the first table for storing remote entities that have a confirmed connection identifier" and "a second [hash] table of unverified remote entities, the second table for storing remote entities that do not have a confirmed connection identifier," especially where the first hash table is populated by a first hash function and where the second hash table is populated by "a second hash function that is cryptographically secure, [having] a lower probability than the first hash function of generating an identical hash for connection identifier information from more than one remote entity" to prevent DoS attacks.

Because of at least the foregoing distinctions, the Applicants submit that the cited art fails to teach or suggest all the limitations of the claims as now recited and therefore rejections under 35 U.S.C. § 103 would be improper and should be withdrawn. Accordingly the Applicants respectfully request favorable reconsideration of the claims as now presented.

In view of the foregoing, Applicant respectfully submits that all the rejections to the independent claims are now moot and that the independent claims are now allowable over the cited art, such that any of the remaining rejections and assertions made, particularly with respect to all of the dependent claims, do not need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice, and particularly with regard to the dependent claims.[4]

[4] Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting any official notice taken.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at 801-533-9800.

Dated this 10th day of February, 2009.

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
THOMAS M. BONACCI
Registration No. 63,368
Attorneys for Applicant
Customer No. 47973

RDN:JCJ:KC:TMB:crb
2269852_1